Codes correcteurs sur des anneaux de Öre multivariés

Lionel Chaussade

Codes correcteurs sur des anneaux de Öre multivariés

L. Chaussade*

30 octobre 2008

Résumé

On étudie dans ce papier certains anneaux de Öre multivariés sur un corps fini. L'adaptation de l'algorithme de Buchberger dans ce cadre non commutatif permet de manipuler les idéaux de ces anneaux, notamment les idéaux bilatères. Ces outils permettent de construire et d'étudier des codes tordus sur ces anneaux de polynômes multivariés et en particulier de fournir la matrice génératrice du code sous forme systématique.

Table des matières

*IRMAR (UMR 6625), Université de Rennes 1, Campus de Beaulieu, F-35042 Rennes Cedex. Doctorant sous la direction de Félix Ulmer.

1 Introduction

Les codes correcteurs cycliques sont vus comme des idéaux de $\mathbb{F}_q[X]/(X^n-1)$ et de manière plus générale, il est possible de regarder les codes construits comme des idéaux de $\mathbb{F}_q[X]/(f)$ où f est un polynôme arbitraire. Bien sûr, dans cette généralisation, la condition simple de stabilité par décalage circulaire des mots du code associé devient un peu plus compliquée.

Pour étendre encore cette construction, si l'on prend un automorphisme, θ, du corps fini $\mathbb{F}_q$, on peut regarder l'anneau de polynômes non commutatif :

$$\mathbb{F}_q[X,\theta] = \{a_0 + ... + a_n X^n,\ a_i \in \mathbb{F}_q\}$$

On additionne ces polynômes de manière usuelle, par contre la multiplication est définie en étendant par associativité et distributivité la règle simple suivante :

$$\forall a \in \mathbb{F}_q,\ Xa = \theta(a)X$$

Ce type d'anneau est un cas particulier des anneaux que Öre a étudié dans [1].

De manière similaire aux codes cycliques dans le cas commutatif, il est possible de définir, en utilisant des idéaux, l'équivalent dans le cadre non commutatif : les θ-codes.

La définition et l'étude des θ-codes a été faite dans [2], [3], [4] et [5].

Le but de ce papier est de présenter une généralisation des θ-codes dans le cas où l'anneau de Öre sous-jacent est un anneau de polynômes à plusieurs variables.

Dans le cas commutatif, une étude des codes correcteurs vus comme des idéaux d'anneaux de polynômes multivariés a été faite dans [6].

On va d'abord étudier les propriétés de ces anneaux de Öre multivariés, ensuite nous verrons que la théorie des bases de Gröbner s'adapte bien et naturellement à ces anneaux de polynômes. L'introduction des bases de Gröbner nous permettra de manipuler les idéaux de cet anneau, notamment les idéaux bilatères. Enfin nous verrons une manière d'obtenir des codes correcteurs grâce aux outils étudiés ainsi que quelques exemples et résultats sur les paramètres du code, notamment une façon d'obtenir la matrice génératrice du code sous forme générique.

2 Etude d'un anneau polynomial de Öre

2.1 Définition

On se place dans $\mathbb{F}_q$ un corps fini de caractéristique p tel que $p^r = q$. Soit $n \geq 2$, on choisit n automorphismes de $\mathbb{F}_q$, $\theta_1, ..., \theta_n$, non nécessairement distincts. On définit de manière ensembliste :

$$\mathbb{F}_q[X_1^{\theta_1}, ..., X_n^{\theta_n}] = \{ \sum_{i_1,...,i_n} a_{i_1,...,i_n} X_1^{i_1} ... X_n^{i_n},\ a_{i_1,...,i_n} \in \mathbb{F}_q\}$$

Cet ensemble est celui des polynômes à n indéterminées à coefficients dans l'anneau $\mathbb{F}_q$. Afin d'alléger les notations, on appellera cet anneau $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]$ et un élément générique sera noté :

$$\sum_{\alpha} a_\alpha X^\alpha$$

où α est un multi-indice.

On va munir cet ensemble d'une structure d'anneau non commutatif. On garde l'addition usuelle mais la multiplication est définie par la règle simple suivante :

$$\forall a \in \mathbb{F}_q,\ \forall i \in \{1, ..., n\},\ X_i a = \theta_i(a) X_i$$

On étend cette règle par associativité et distributivité. On suppose que les variables X_i commutent. La multiplication devient alors bien définie, de manière plus précise :

$$(\sum_{\alpha} a_\alpha X^\alpha)(\sum_{\beta} b_\beta X^\beta) = \sum_{\alpha,\beta} a_\alpha \theta^\alpha(b_\beta) X^{\alpha+\beta}$$

On utilise ici la notation suivante : si $\alpha = (\alpha_1, ..., \alpha_n)$ alors $\theta^\alpha = \theta_1^{\alpha_1}...\theta_n^{\alpha_n}$ où la loi utilisée est la composition des automorphismes.

On a donc défini un anneau de polynômes à plusieurs variables non commutatif, $\mathbb{F}_q[\underline{X^\theta}]$. Voyons quelques propriétés de cet anneau.

2.2 Propriétés

Proposition 1 *L'anneau $\mathbb{F}_q[\underline{X^\theta}]$ est unitaire, intègre et ses éléments inversibles sont les inversibles de $\mathbb{F}_q$.*

Preuve :
On peut voir l'intégrité en utilisant le degré total et en remarquant que le degré total d'un produit est égal à la somme des degrés totaux de chacun des facteurs. La caractérisation des inversibles de cet anneau est également évidente.

□

Par analogie avec le cas à une variable, on va étudier les codes correcteurs qui sont des idéaux de $\mathbb{F}_q[\underline{X^\theta}]/I$ où I est un idéal de $\mathbb{F}_q[\underline{X^\theta}]$. Pour que ce quotient ait une structure d'anneau, il convient que I soit un idéal bilatère. Si un idéal est engendré par des éléments centraux, alors il est en particulier bilatère. C'est pour cette raison que l'étude des éléments centraux de $\mathbb{F}_q[\underline{X^\theta}]$ nous intéresse.

Proposition 2 *On a l'inclusion suivante :*

$$\{ \sum_{i_1,...,i_n} a_{i_1,...,i_n} X_1^{i_1|<\theta_1>|}...X_n^{i_n|<\theta_n>|},\ a_{i_1,...,i_n} \in \bigcap_{i=1}^{n} (\mathbb{F}_q)^{\theta_i} \} \subset Z(\mathbb{F}_q[\underline{X^\theta}])$$

où $Z(\mathbb{F}_q[\underline{X^\theta}])$ désigne le centre de l'anneau $\mathbb{F}_q[\underline{X^\theta}]$ et $|<\theta_i>|$ l'ordre de l'automorphisme θ_i.

Preuve :
Il suffit de voir par distributivité et associativité que les éléments dans l'ensemble du membre de gauche commutent avec les constantes et les X_i. Ceci est immédiat à vérifier.

□

Cela signifie que certains éléments centraux ont une forme particulièrement simple qui généralise assez naturellement le cas à une variable. On nommera par la suite ces éléments centraux particulier les polynômes super-centraux. Lorsque nous travaillerons avec des idéaux bilatères, nous les chercherons très souvent engendrés par des polynômes super-centraux. Nous verrons dans l'annexe 2 à quoi ressemble plus précisément l'ensemble des éléments centraux, puisque l'inclusion de la proposition précédente est en générale stricte.

On va être amené à travailler avec des idéaux et des quotients dans des anneaux à plusieurs indéterminées. Dans le cas commutatif, pour de tels calculs, l'utilisation des bases de Gröbner est incontournable. Nous allons voir dans le chapitre suivant que les principales propriétés des bases de Gröbner s'adaptent dans notre cas de manière assez simple.

3 Bases de Gröbner dans le cas non commutatif

Les bases de Gröbner dans les anneaux de Öre ont été étudiées en toute généralité dans [7] et [9]. Une approche concernant les bases de Gröbner dans les idéaux bilatères est faite dans [8]. Ici le cadre dans lequel on travaille est assez particulier puisque l'anneau de Öre $\mathbb{F}_q[\underline{X^\theta}]$ ne comporte pas de dérivation. Une théorie simple des bases de Gröbner peut alors être mise en place. Elle calque la théorie classique du cas commutatif avec des adaptations mineures.

Avant tout, il convient de dire un mot sur les ordres monomiaux. En fait, sur ce point là, il n'y a pas de différence entre le cas commutatif et le cas non commutatif. Un ordre monomial classique sera également un ordre monomial de $\mathbb{F}_q[\underline{X}^{\theta}]$. Dans la suite, si ce n'est pas précisé, c'est l'ordre lexicographique (avec $X_1 > ... > X_n$) qui sera utilisé. Une présentation détaillée des différents ordres monomiaux est faite dans [11] page 52.

3.1 Introduction

Le but est d'arriver au résultat suivant qui est analogue au cas commutatif que l'on retrouve par exemple dans [11] page 79.

Theorème 1 *Soit J un idéal à gauche de $\mathbb{F}_q[\underline{X}^{\theta}]$. Il existe $G = \{g_1, ..., g_t\}$ qui engendre à gauche l'idéal J tel que pour tout $f \in \mathbb{F}_q[\underline{X}^{\theta}]$, il existe un unique $r \in \mathbb{F}_q[\underline{X}^{\theta}]$ vérifiant les deux conditions suivantes :*

- *Il existe $g \in J$ tel que $f = g + r$.*
- *Aucun des monômes de r n'est divisible par un des monômes de tête des g_i.*

Il faut bien faire attention au fait que les idéaux que l'on considère sont des idéaux à gauche.

3.2 Les S-polynômes

Un outil classique des bases de Gröbner est la notion de S-polynôme. C'est juste un polynôme créé à partir de deux autres qui a pour but de faire s'annuler les termes dominants. Il convient dans notre contexte particulier d'adapter un peu la définition afin que les termes dominants s'annulent encore malgré l'action des automorphismes.

Definition 1 *Soit $(f, g) \in \mathbb{F}_q[\underline{X}^{\theta}]^2$ ayant pour termes dominants respectivement $aX_1^{\alpha_1}...X_n^{\alpha_n}$ et $bX_1^{\beta_1}...X_n^{\beta_n}$. Posons $\gamma_i = Max(\alpha_i, \beta_i)$. On pose $\alpha = (\alpha_1, ..., \alpha_n)$ et de même on définit β et γ. Le S-polynôme de f et g est donné par la formule suivante :*

$$S(f, g) = \frac{1}{\theta^{\gamma-\alpha}(a)} X^{\gamma-\alpha} f - \frac{1}{\theta^{\gamma-\beta}(b)} X^{\gamma-\beta} g$$

C'est donc bien un polynôme fabriqué pour simplifier les termes de tête de f et g.

Il est également important de remarquer que $S(f, g)$ appartient à l'idéal à gauche engendré par f et g puisque que l'on n'a effectué que des multiplications à gauche.

3.3 L'algorithme de Buchberger

Mise à part cette petite adaptation nécessaire pour les polynômes tordus, le reste fonctionne exactement pareil que dans le cas commutatif. On obtient l'algorithme suivant qui peut être implémenté en Magma et qui permet de calculer une base de Gröbner d'un idéal à gauche.

1) On part de notre idéal à gauche, J, engendré par $(f_1, ..., f_r)$. On calcule les $S(f_i, f_j)$ pour i distinct de j.

2) On calcule un des restes de $S(f_i, f_j)$ dans la division à droite par la famille $(f_1, ..., f_r)$. Si un de ces restes, S, est non nul alors on transforme $(f_1, ..., f_r)$ en $(f_1, ..., f_r, S)$.

3) On recommence l'algorithme à l'étape 1.

4) On réduit la base de Gröbner ainsi obtenue et on la normalise comme dans le cas commutatif.

On obtient alors une base de Gröbner de l'idéal I qui a les propriétés énoncées dans le théorème.

Exemple 1 :
Voyons pas à pas sur un exemple comment marche cet algorithme. Soient $\theta(x) = x^2$ et α le générateur de $\mathbb{F}_4$ donné par Magma. Soit J l'idéal de $\mathbb{F}_4[X^\theta, Y^\theta]$ engendré à gauche par :

$$f_1 = X^2Y + X^2 + 1,\ f_2 = X^2Y^2 + \alpha X + 1$$

On a $S(f_1, f_2) = X^2Y + \alpha X + Y + 1$ et son reste dans la division par $< f_1, f_2 >$ est non nul et vaut :

$$f_3 = X^2 + \alpha X + Y$$

On poursuit l'algorithme en calculant $S(f_1, f_3) = X^2 + \alpha XY + Y^2 + 1$, son reste dans la division par l'idéal à gauche $< f_1, f_2, f_3 >$ vaut :

$$f_4 = \alpha^2 XY + \alpha X + Y^2 + Y + 1$$

On a $S(f_2, f_3) = \alpha XY^2 + \alpha X + Y^3 + 1$ dont le reste est nul dans la division par $< f_1, f_2, f_3, f_4 >$ on passe donc à l'étape suivante.

Au final, on obtient $J =< f_1, f_2, f_3, f_4, \alpha^2 X + \alpha Y^3 + Y^2 + \alpha Y + \alpha, \alpha Y^5 + \alpha^2 Y^4 + \alpha^2 Y^3 + \alpha Y^2 + \alpha^2 Y, Y^4 + Y^3, \alpha Y^2 + Y, \alpha Y >$Au L'étape de la réduction de la base consiste à ne garder que les polynômes dont les termes de tête ne sont multiples d'aucun autre terme de tête de polynômes de la famille obtenue, il reste donc :

$$J =< \alpha^2 X + \alpha Y^3 + Y^2 + \alpha Y + \alpha, \alpha Y >$$

Enfin on normalise la base et on obtient une base de Gröbner de J qui est :

$$J =< X + \alpha^2 Y^3 + \alpha Y^2 + \alpha^2 Y + \alpha^2, Y >$$

Remarque :
Dans cet algorithme, on utilise la division d'un polynôme par une famille de polynômes. Cet algorithme se passe comme dans le cas commutatif, c'est-à-dire que l'on essaie de faire s'annuler le terme de tête du polynôme à diviser à l'aide des termes de tête des diviseurs. Lorsque qu'on ne le peut pas, on met le monôme récalcitrant dans le reste. Bien sûr cette division n'est pas unique (c'est pour cela que les bases de Gröbner existent) et peut donner plusieurs restes en fonction de la manière dont on s'y prend.

Exemple 2 : Voici à présent un exemple que l'on va garder en fil rouge durant ce papier pour illustrer les différentes notions que l'on va introduire. On se place dans $\mathbb{F}_4[X^\theta, Y^\theta]$ où $\theta(x) = x^2$ muni de l'ordre lexicographique. On note écrit $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ où α est le générateur de $\mathbb{F}_4$ donné par Magma. Soit J l'idéal à gauche engendré par $\{f, g\}$ avec :

$$f = X^2Y^4 + X^2,\ g = X^3Y^2 + \alpha Y$$

Une base de Gröbner minimale est donnée par les polynômes p, q et r avec :

$$p = Y^5 + Y,\ q = X^2Y^4 + X^2,\ r = X^4 + \alpha Y^3$$

Voyons une première utilisation des bases de Gröbner dans notre contexte.

4 Degré et borne d'un idéal

4.1 Degré d'un idéal

Definition 2 *On appelle degré de l'idéal à gauche J la dimension de $\mathbb{F}_q[\underline{X^\theta}]/J$ en tant que $\mathbb{F}_q$-espace vectoriel.*

Remarques :

• Même si J n'est pas un idéal bilatère et que le quotient $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]/J$ n'a donc pas forcément une structure d'anneau, c'est bien un espace vectoriel sur $\mathbb{F}_q$.

• Cette dimension peut être infinie, mais dans notre contexte pour faire des codes correcteurs, on va vouloir se placer dans le cas où la dimension est finie.

Voyons à présent un moyen rapide de voir si la dimension de $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]/J$ est finie et de la calculer.

Soit J un idéal à gauche et $(g_1, ..., g_r)$ une base de Gröbner de J. Puisque le reste dans la division par J est uniquement déterminé lorsque l'on utilise une base de Gröbner, on peut identifier l'ensemble des classes modulo J à l'ensemble des restes. Un reste a la propriété de n'avoir aucun monôme divisible par l'un des termes de tête des g_i. La dimension de $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]/J$ en tant que $\mathbb{F}_q$-espace vectoriel est égal au cardinal de

$$\{X^\alpha,\ X^\alpha \notin < LM(g_1), ..., LM(g_r) >\}$$

où $LM(g_i)$ désigne le monôme de tête de g_i. Notons $D(J)$, cette dimension.

Proposition 3 *Soit J un idéal et $(g_1, ..., g_t)$ une base de Gröbner de J. Alors $D(J)$ est finie si et seulement s'il existe $(i_j)_{1\leq j\leq n}$ tels que $LM(g_{i_j}) = X_j^{a_j}$ avec a_j des entiers strictement positifs.*

Preuve :

Soit $n \geq 2$. Notons $LM(g_i) = X_1^{a_{i,1}}...X_n^{a_{i,n}}$. Supposons par l'absurde que, par exemple, $\forall i,\ a_{i,1} > 0$, alors la famille de monômes $(X_n^j)_{j\geq 0}$ n'appartient pas à $< LM(g_1), ..., LM(g_r) >$. La dimension de $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]/J$ sera alors infinie.

Réciproquement prenons le plus petit entier a_j tel qu'il existe i avec $LM(g_i) = X_j^{a_j}$. Une famille génératrice de $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]/J$ est $\{X_1^{i_1}...X_n^{i_n}\}_{0\leq i_j\leq a_j-1}$ qui est bien de cardinal fini.

□

Exemple :

Si l'on reprend l'exemple précédent, on a l'idéal donné par sa base de Gröbner :

$$J =< Y^5 + Y, X^2Y^4 + X^2, X^4 + \alpha Y^3 >$$

D'après la proposition précédente, on voit donc immédiatement que $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]/J$ est de dimension finie.

Celle-ci vaut 18 et une base du quotient est donnée par les monômes suivants :

$$\{Y^0, Y, ..., Y^4, XY^0, ..., XY^4, X^2Y^0, ..., X^2Y^3, X^3Y^0, ..., X^3Y^3\}$$

C'est-à-dire l'ensemble des monômes qui ne sont pas divisibles par l'un des termes de tête des éléments de la base de Gröbner.

Un des intêrets du calcul d'une base de Gröbner est de pouvoir connaître rapidemment le degré d'un idéal et pouvoir faire des opérations dans le quotient $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]/J$ qui a maintenant une base naturelle.

Remarque :

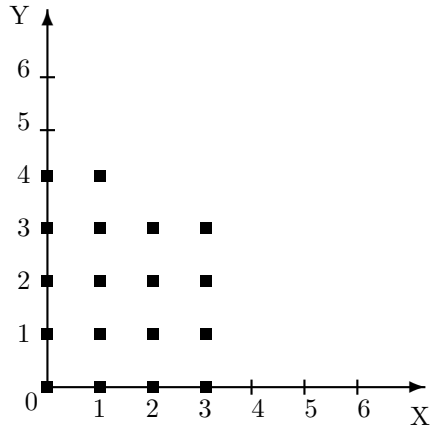
Par la suite, on va donc chercher des idéaux à gauche de degré fini.

On peut remarquer tout de suite que si J est engendré à gauche par un seul élément alors le degré de J vaut 0 (cas trivial) ou est infini.

4.2 Vision sous forme d'escalier

Il existe une manière visuelle de représenter une base du quotient $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]/J$.
Reprenons l'exemple précédent, on a alors l'escalier associé à l'idéal :

$$J =< Y^5 + Y, X^2Y^4 + X^2, X^4 + \alpha Y^3 >$$



Dans ce diagramme un carré se trouve à la position (i, j) si et seulement si X^iY^j est un monôme qui n'est divisible par aucun des termes de tête de la base de Gröbner réduite de J. Ceci est équivalent à dire que le monôme en question est un élément de la base naturelle de $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]/J$.
Dans cet exemple, on retrouve le fait que la dimension en tant que $\mathbb{F}_q$-espace vectoriel de $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]/J$ est finie est vaut 18.

Remarque :
Si $J \subset J'$ sont deux idéaux à gauche alors l'escalier de J contient l'escalier de J'. La réciproque est vraie pour des idéaux monomiaux mais fausse en général.

4.3 Existence d'une borne

Dans la construction des codes tordus classique, le polynôme générateur du code, g, doit être un diviseur à droite d'un polynôme central f. Ce qui dans le langage des idéaux se traduit par le fait que l'idéal à gauche (g) contient l'idéal bilatère (f).

Afin de généraliser cette approche, on est donc amené à étudier le problème suivant : étant donné J un idéal à gauche, existe-il toujours un idéal bilatère I inclus dans J tel que I soit de degré fini ?

Definition 3 *Soit J un idéal à gauche de $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]$, on dit que I est une borne pour J si $I \subset J$ et I bilatère.*

Proposition 4 *Tout idéal à gauche de degré fini possède une borne.*

Preuve :
Soit J un idéal à gauche et $G = (f_1, ..., f_r)$ une base de Gröbner de J. Montrons que J contient un élément central. D'après la propriété sur les bases de Gröbner, pour tout $i \geq 0$, on effectue la division suivante :

$$X_1^{i|<\theta_1>|} = A_i + R_i$$

où $A_i \in J$ et R_i est le reste.

Comme le degré de J est fini par hypothèse, ces restes appartiennent à un sous-espace vectoriel sur $\mathbb{F}_q$ de dimension finie (l'espace vectoriel dont une base est formée des monômes qui ne sont pas dans l'idéal engendré par les monômes de tête des f_i). Cet espace vectoriel est également de dimension finie sur $\mathbb{F}_p$ où p est la caractéristique de $\mathbb{F}_q$. Il existe donc $d \in \mathbb{N}$ et $(d_i)_{0 \leq i \leq d} \in \mathbb{F}_p$ tels que :

$$\sum_{i=0}^{d} d_i R_i = 0$$

En effectuant la même combinaison linéaire sur les divisions écrites au dessus, on obtient alors :

$$\sum_{i=0}^{d} d_i X_1^{i|<\theta_1>|} \in J$$

On a trouvé un élément central dans J, donc $< \sum_{i=0}^{d} d_i X_1^{i|<\theta_1>|} > \subset J$. On pose $I =< \sum_{i=0}^{d} d_i X_1^{i|<\theta_1>|} >$, c'est bien une borne pour J.

□

Cependant, ce qui nous intéresse est que la borne I soit également de degré fini et c'est possible :

Proposition 5 *Tout idéal de degré fini possède une borne de degré fini.*

Preuve :

Soit J un idéal de degré fini. Ce que l'on a fait dans la preuve précédente avec la variable X_1, on peut le recommencer avec les autres variables, c'est-à-dire qu'il existe des polynômes $P_i \in \mathbb{F}_p[X_i^{|<\theta_i>|}]$ (ils sont donc centraux) appartenant à l'idéal J. Posons $I =< P_1, ..., P_n >$. Nous allons montrer que I est bien une borne de degré fini de J. Déjà, il est clair que I est inclus dans J et que c'est un idéal bilatère.

Remarquons ensuite que lorsque l'on effectue la division d'un élément f par l'idéal I, le reste ne contient aucun monôme divisible par l'un des termes dominants des P_i. C'est-à-dire que la dimension de $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]/I$ est au plus $\prod_{i=1}^{n} Deg_{X_i}(P_i)$.

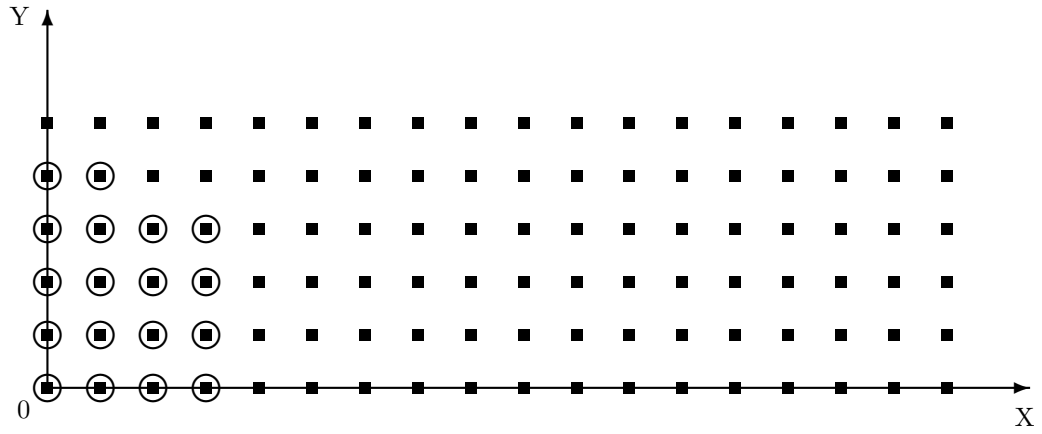
□

Exemple :

Reprenons toujours notre exemple précédent, avec J donné à l'aide d'une base de Gröbner par $J =< Y^5 + Y, X^2Y^4 + X^2, X^4 + \alpha Y^3 >$.

En effectuant plusieurs divisions successives et en cherchant des relations linéaires, on trouve $P_1 = X^{18} + X^2$ et $P_2 = Y^6 + Y^2$ qui appartiennent à J. L'idéal $I =< X^{18} + X^2, Y^6 + Y^2 >$ est bien un idéal bilatère inclus dans J et il est de degré fini, $108 = 18 \times 6$.

Voici le graphique représentant l'escalier de J et l'escalier de I. L'escalier de I contient donc celui de J :



Les cercles représentent l'escalier et J et les carrés celui de I.

4.4 Borne de degré minimale

Le diagramme précédent montre que la borne I donnée par l'algorithme peut être, dans certains cas, assez grossière. On se pose naturellement la question suivante : étant donné un idéal à gauche J peut-on trouver un idéal bilatère $I \subset J$ tel que le degré de I soit minimum ?

En effet, on voit que choisir I engendré par un polynôme en X et un polynôme en Y est assez restrictif, il est fort possible qu'il y ait des polynômes mélangeant les variables X et Y qui soient centraux et qui appartiennent à J. En particulier l'un des défauts de la construction de l'exemple précédent est que l'escalier de I ne tient pas compte de la forme particulière de l'escalier de J.

Par la suite le degré de la borne I va correspondre à la longueur du code correcteur, il est donc intéressant d'essayer d'optimiser ce degré.

L'algorithme suivant permet de trouver des polynômes centraux inclus dans J :

1) Soit J un idéal à gauche de degré fini, k, donné par une base de Gröbner et soit $(N_1, ..., N_n) \in \mathbb{N}^n$.

2) Pour tous les entiers $(i_1, ..., i_n) \in [0...N_1 - 1] \times ... \times [0...N_n - 1]$, on effectue la division de $X_1^{i_1|<\theta_1>|}...X_n^{i_n|<\theta_n>|}$ par l'idéal J :

$$X_1^{i_1|<\theta_1>|}...X_n^{i_n|<\theta_n>|} = A_{i_1,...,i_n} + R_{i_1,...,i_n}$$

où $A_{i_1,...,i_n} \in J$.

D'après la propriété fondamentale sur les bases de Gröbner, les restes $R_{i_1,...,i_n}$ ne sont composés que de monômes non divisibles par l'un des monômes de tête des générateurs de la base de Gröbner de J. On peut donc convertir les $R_{i_1,...,i_n}$ en des vecteurs de taille k à coefficients dans $\mathbb{F}_q$.

3) On forme la matrice en mettant en colonnes les $N_1...N_n$ vecteurs ainsi obtenus et l'on voit cette matrice comme une application $\cap_{i=1}^n (\mathbb{F}_q)^{\theta_i}$-linéaire. On cherche une base du noyau de cette matrice. Un élement de ce noyau, nous fournit donc une relation de dépendance linéaire entre les $R_{i_1,...,i_n}$ à coefficients dans $\cap_{i=1}^n (\mathbb{F}_q)^{\theta_i}$. En effectuant la même relation de dépendance linéaire sur les divisions de l'étape 2 on obtient un polynôme central qui appartient à J.

On peut faire varier les N_i et les fixer de plus en plus grands pour obtenir d'autres polynômes centraux.

4) On forme l'idéal bilatère I engendré par les polynômes centraux ainsi trouvés.

Remarque Si l'on prend $N_i \geq \frac{deg(P_i)}{|<\theta_i>|}$ alors les polynômes P_i de la proposition 5 vont être pris en compte par l'algorithme précédent, ainsi on sera assuré que l'idéal I trouvé est bien de degré fini.

Definition 4 *Soit J un idéal à gauche de degré fini. On appelle idéal bilatère maximal associé à J et on note I^* l'idéal engendré par l'ensemble des polynômes centraux appartenant à J.*

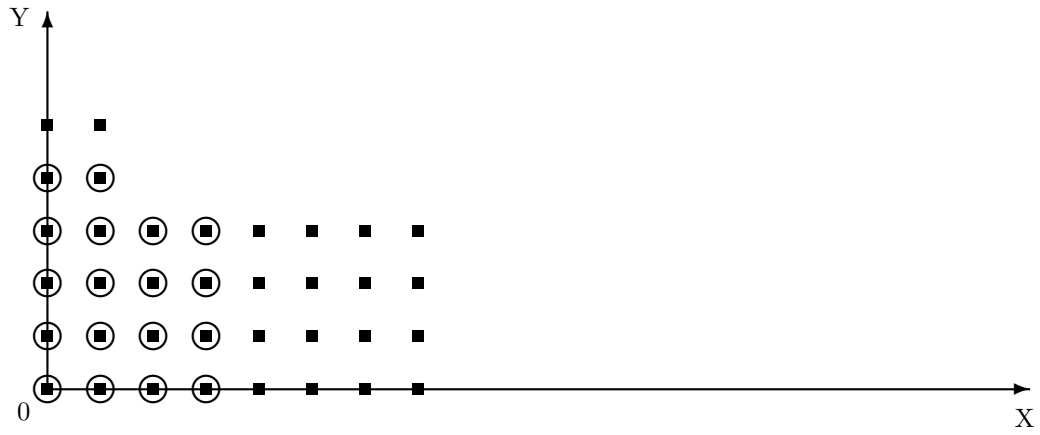
On va, dans les exemples que l'on va considérer par la suite, prendre les N_i suffisamment grand afin d'avoir un idéal I assez proche de J sans forcément être l'idéal bilatère maximal associé à J.

Exemple :
Revenons à notre exemple précédent, c'est-à-dire $J =< Y^5 + Y, X^2Y^4 + X^2, X^4 + \alpha Y^3 >$, on avait trouvé une borne pour J de degré 108, en fait il est possible de faire mieux en utilisant l'algorithme décrit précédemment.

Avec $N_1 = N_2 = 10$, on trouve un certain nombre de polynômes centraux inclus dans J une base de Gröbner de l'idéal engendré par les polynômes centraux ainsi obtenus est :

$$I =< Y^6 + Y^2, X^2Y^4 + X^2, X^8 + Y^2 >$$

Le degré de I est 36, de plus si l'on dessine les escaliers correspondants aux idéaux I et J, on voit que la forme de I est moins grossière et mieux adaptée à l'idéal J que précédemment.



4.5 Base de Gröbner pour les idéaux bilatères

Afin de travailler avec l'idéal I on est amené à calculer une base de Gröbner d'un idéal engendré par des polynômes centraux. Remarquons tout de suite la propriété suivante :

Proposition 6 *Soit $I =< f_1, ...f_r >$ un idéal où les f_i sont super-centraux et soit $I =< g_1, ..., g_t >$ une base de Gröbner de I, alors les g_i sont super-centraux.*

Preuve :
Pour montrer cela remarquons deux choses :
• Le S-polynôme de deux polynômes super-centraux est super-central (ce qui est évident si l'on regarde la formule des S-polyômes).
• Lorsque l'on effectue l'algorithme de division d'un polynôme super-central par d'autre polynômes super-centraux, le reste est un polynôme super-central. En effet tout se passe comme si l'on travaillait dans l'anneau $(\cap_{i=1}^{n}(\mathbb{F}_q)^{\theta_i})[X_1^{|<\theta_1>|}, ..., X_n^{|<\theta_n>|}])$.

□

Nous avons à présent tous les outils pour voir comment fabriquer un code correcteur à l'aide de ces anneaux de Öre multivariés.

5 Fabrication de codes

5.1 Propriétés sur les mots du code

Soit J un idéal à gauche de $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]$ de degré fini et I une borne de J de degré fini n. Après avoir pris une base de Gröbner pour I, il existe une base naturelle du quotient $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]/I$ qui est de cardinal n. Par le théorème de la correspondance des idéaux, J peut être vu comme un idéal à gauche de $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]/I$ puisqu'il contient I. A chaque polynôme de l'idéal, on associe alors un mot de $\mathbb{F}_q^n$ dont les composantes sont juste les coordonnées du polynôme dans la base de $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]/I$.

Il y a ainsi une application qui à un idéal de $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]/I$ associe un code sur $\mathbb{F}_q$. C'est une généralisation naturelle de la construction des θ-codes. Néanmoins si l'on traduit en terme de mots du code la stabilité par multiplication à gauche par X_i, on obtient des propriétés bien particulières du code.

Voyons à quoi ressemblent ces propriétés que l'on a sur les mots dans un exemple simple.

Exemple :
Prenons un exemple simplifié (cas des codes multi θ-cycliques).
Soit J un idéal à gauche de $\mathbb{F}_q[X^{\theta_1}, Y^{\theta_2}]/(X^r - 1, Y^s - 1)$.
Si $P \in J$ avec :

$$P = a_{0,0} + a_{0,1}Y + ... + a_{0,s-1}Y^{s-1} + a_{1,0}X... + a_{r-1,s-1}X^{r-1}Y^{s-1}$$

alors

$$XP = \theta(a_{0,0})X + \theta(a_{0,1})XY + ... + \theta(a_{0,s-1})XY^{s-1} + \theta(a_{1,0})X^2... + \theta(a_{r-1,s-1})Y^{s-1}$$

Donc finalement la stabilité par multiplication par X se traduit par la condition suivante sur les mots du code C :

$$(a_{0,0}, a_{0,1}, ...a_{0,s-1}, a_{1,0}, a_{1,1}, ..., a_{1,s-1}, ...a_{r-1,0}, a_{r-1,1}, ...a_{r-1,s-1}) \in C$$

$$\Longleftrightarrow$$

$$(\theta(a_{r-1,0}), ..., \theta(a_{r-1,s-1}), \theta(a_{0,0}), ...\theta(a_{0,s-1}), ..., \theta(a_{r-2,0}), ..., \theta(a_{r-2,s-1})) \in C$$

En fait c'est comme si le code était cyclique par blocs.

Si l'on traduit à présent la condition de stabilité par multiplication par Y, on obtient la condition suivante sur les mots :

$$(a_{0,0}, a_{0,1}, ...a_{0,s-1}, a_{1,0}, a_{1,1}, ..., a_{1,s-1}, ...a_{r-1,0}, a_{r-1,1}, ...a_{r-1,s-1}) \in C$$

$$\Longleftrightarrow$$

$$(\theta(a_{0,s-1}), ..., \theta(a_{0,s-2}), \theta(a_{1,s-1}), ..., \theta(a_{1,s-2}), ...\theta(a_{r-1,s-1}), ...\theta(a_{r-1,s-2})) \in C$$

C'est-à-dire qu'à l'intérieur de chacun des r blocs de taille s, il y a un décalage circulaire. On peut appeler ce code multi θ-cyclique.

Ici c'est un cas assez simple où les polynômes de l'idéal ont une forme assez agréable. Dans le cas général, même s'il y a des décalages circulaires sur les blocs et à l'intérieur des blocs, ces décalages sont perturbés par l'apparition de nouveaux termes comme dans le cas des θ-codes qui ne sont pas θ-cycliques.

5.2 Algorithme utilisé

Voici les étapes de l'algorithme mis en oeuvre pour obtenir les exemples de codes qui vont suivre.

1) On se place dans $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]$ (qui sera souvent $\mathbb{F}_4[X^\theta, Y^\theta]$). On choisit un idéal à gauche J. En pratique, on prendra souvent J engendré par deux polynômes.

2) On calcule la base de Gröbner réduite de J. Grâce à cette base de Gröbner, on peut connaître le degré de J. Si $0 < D(J) < +\infty$ on continue, sinon on choisit un autre idéal.

3) On calcule une borne pour J, que l'on note I à l'aide de l'algorithme présenté dans le chapitre précédent.

4) On voit les éléments de $J \subset \mathbb{F}_q[\underline{X}^{\underline{\theta}}]/I$ comme des $D(I)$-uplets qui forment les mots d'un code.

Nous allons voir tout de suite un moyen simple de prévoir les paramètres du code ainsi obtenu et surtout d'avoir facilement la matrice génératrice sous forme systématique du code.

6 Dimension du code et matrice génératrice

Le but de ce paragraphe est de montrer que l'on peut prévoir la dimension du code que l'on obtient.

6.1 Cadre et notations

Soit J un idéal à gauche de degré k, c'est-à-dire qu'une base de l'espace vectoriel sur $\mathbb{F}_q$, $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]/J$, a pour cardinal k. Notons cette base $E = \{e_1, ..., e_k\}$. On remarque que les éléments de cette base sont des monômes, plus précisément ce sont les monômes qui ne sont pas divisibles par l'un des monômes de tête d'un élément de J (ou de manière équivalente par l'un des monômes de tête des éléments d'une base de Gröbner de J).

Soit $I \subset J$ une borne pour J avec $D(I) = n$. Notons une base de $\mathbb{F}_q[\underline{X}^{\underline{\theta}}]/I$ en tant que $\mathbb{F}_q$-espace vectoriel $F = \{e_1, ..., e_k, f_1, .., f_{n-k}\}$. On peut choisir une base de cette forme là comme $I \subset J$ (en effet les monômes qui ne sont divisibles par aucun des termes de tête des éléments de J ne sont, à fortiori, divisibles par aucun des termes de tête des éléments de I). On note C le code correcteur ainsi obtenu.

6.2 Résultat

On a la proposition suivante sur la dimension du code C.

Proposition 7 *La dimension de C est $n - k$.*

Remarque :
Comme attendu cela correspond à ce qui se passe pour les codes tordus en une variable. En effet si g est le polynôme générateur du code de degré k et f une borne de degré n, on sait que le code a pour dimension $n - k$.

Preuve :
Le code C est formé de l'ensemble des restes des éléments de J dans la division par I.
Montrons pour commencer que $dim(C) \geq n - k$.

En conservant les notations du préambule, effectuons la division de f_i par l'idéal J :

$$f_i = R_i - \sum_{j=1}^{k} \beta_i^j e_j$$

où $R_i \in J$ donc

$$R_i = f_i + \sum_{j=1}^{k} \beta_i^j e_j$$

est un élément de J. Regardons à quel mot du code il correspond, c'est-à-dire quel est son reste dans la division par I. On a :

$$R_i = 0 + R_i$$

en effet les monômes de R_i font partie de la base F.

En écrivant les coordonnées dans la base F, on a donc le mot suivant qui appartient à C :

$$(\beta_i^1, ..., \beta_i^k, \delta_i^1, ..., \delta_i^{n-k})$$

où δ est le symbole de Kronecker.

La dimension de C est donc au moins $n - k$.

La base de F n'est peut être pas rangée par ordre lexicographique mais une permutation de la base ne change pas le résultat sur la dimension du code.

Montrons à présent que la dimension du code est exactement $n - k$.

Pour cela montrons que $Vect\{e_1, ..., e_k\} \cap C = \{0\}$ et cela nous permettra de conclure d'après la formule des dimensions de Grassman.

Soit m appartenant à l'intersection, il existe donc $P \in J$ tel que :

$$P = R + m$$

où $R \in I$.

Donc $m = P - R$ est dans J. C'est absurde au vu des monômes que comprend m sauf si $m = 0$.

D'où le résultat.

□

Remarque :

• Grâce à la forme du mot de code correspondant à R_i, on remarque que la distance minimale de C vérifie :

$$d(C) \leq k + 1$$

Ce qui correspond à la borne de Singleton.

La méthode précédente va nous permettre de former une matrice génératrice et une matrice de parité du code.

6.3 Matrice génératrice

Dans la démonstration du chapitre précédent, il ressort que les mots :

$$c_i = (\beta_i^1, \beta_i^2, ..., \beta_i^k, \delta_i^1, ..., \delta_i^{n-k})$$

forment une base du code. Si l'on change l'ordre de la base en $(f_1, ..., f_{n-k}, e_1, ..., e_k)$ et que l'on met chacun des mots de la base du code en ligne, on obtient donc la matrice génératrice suivante de taille $(n - k) \times n$:

$$\left(\begin{array}{c|c} Id_{n-k} & (\beta_i^j) \end{array} \right)$$

On remarque que cette matrice génératrice est en fait la matrice génératrice sous forme générique.

6.4 Matrice de parité

Ayant la matrice génératrice sous forme générique, on peut facilement en déduire la matrice de parité, celle ci est de taille $(n-k) \times n$ et s'écrit :

$$\left(\begin{array}{c|c} -\beta_j^i & Id_{n-k} \end{array} \right)$$

7 Exemples

Voyons à présent quelques exemples de codes correcteurs que l'on obtient. On suit la même construction que dans le texte c'est-à-dire que l'on choisit d'abord l'idéal J.

Exemple 1 :
1) On se place dans $\mathbb{F}_4[X^\theta, Y^\theta]$ où $\theta(x) = x^2$.

2) Soient

$$P = \alpha X^2 + \alpha XY^2 + XY + X + \alpha^2 Y^2 + Y + \alpha^2$$
$$Q = \alpha X^2 Y^2 + X^2 Y + \alpha X^2 + XY^2 + X + Y^2 + Y + 1$$

On note $J =< P, Q >$ l'idéal à gauche engendré par P et Q.

3) Une base de Gröbner à gauche engendrée par P et Q est engendrée à gauche par les polynômes suivants :

$$P' = X^2 + XY^2 + \alpha^2 XY + \alpha^2 X + \alpha Y^2 + \alpha^2 Y + \alpha$$
$$Q' = XY + \alpha^2 X + \alpha Y^4 + Y^3 + Y^2 + \alpha^2 Y$$
$$R' = Y^3 + \alpha Y^2 + \alpha^2 Y + 1$$

L'idéal J est donc de degré 4 et une base du $\mathbb{F}_4$-espace vectoriel $\mathbb{F}_4[X^\theta, Y^\theta]/J$ est $\{1, Y, Y^2, X\}$.

4) Si l'on prend $N_1 = N_2 = 10$, on obtient l'idéal I donné avec sa base de Gröbner :

$$I =< X^2 + 1, Y^6 + 1 >$$

On remarque d'ailleurs que ces polynômes ne sont autres que P_1 et P_2.

5) On effectuant les quelques divisions décrites au chapitre précédent, on obtient un code de paramètres $[12, 8, 4]$ sur $\mathbb{F}_4$ qui a pour matrice génératrice sous forme systématique :

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \alpha^2 & \alpha & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^2 & \alpha^2 & \alpha^2 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \alpha^2 & \alpha^2 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & \alpha & \alpha^2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & \alpha^2 & 0 & \alpha^2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & \alpha & \alpha & 1 & \alpha^2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & \alpha & \alpha & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \alpha^2 & \alpha & 0 & \alpha^2 \end{pmatrix}$$

Exemple 2 :

1) Prenons cette fois l'anneau $\mathbb{F}_9[X^\theta, Y^\theta]$ où $\theta(x) = x^3$ muni de l'ordre lexicographique classique. On note α le générateur de $\mathbb{F}_9$ donné par Magma.

2) Soit $J =< f, g >$ l'idéal à gauche engendré par :

$$f = X^2Y^2 + \alpha^7X^2Y + \alpha^2X^2 + XY^2 + \alpha XY + \alpha^6X + \alpha^2Y^2 + \alpha^5Y + \alpha^6$$
$$g = \alpha^6X^2Y^2 + \alpha^3X^2Y + \alpha X^2 + 2XY^2 + \alpha^3XY + X + \alpha^6Y^2 + \alpha Y + \alpha^6$$

3) Une base de Gröbner de J est donnée par :

$$p = X + \alpha^5Y^5 + \alpha Y^4 + Y^3 + Y^2 + \alpha^2$$
$$q = Y^3 + Y^2 + \alpha^2Y + \alpha^2$$

On remarque que J est bien de degré fini.

4) Une borne de degré fini de J est :

$$I =< X^2 + \alpha^3, Y^6 + \alpha^3Y^4 + \alpha^6Y^2 + \alpha^3 >$$

5) On obtient alors un code de paramètres $[12, 9, 3]$ sur $\mathbb{F}_9$.

8 Annexe

Dans la proposition 2, nous avons vu une famille particulièrement simple de polynômes centraux, mais il y en a d'autres. Nous allons dans ce paragraphe décrire complétement le centre de $\mathbb{F}_q[\underline{X^\theta}]$.

Soit $P = \sum_{i_1,...,i_n} a_{i_1,...,i_n} X_1^{i_1}...X_n^{i_n}$ un polynôme central, écrivons ce que signifie la condition $X_jP = PX_j$:

$$\sum_{i_1,...,i_n} \theta_j(a_{i_1,...,i_n}) X_1^{i_1}...X_j^{i_j+1}...X_n^{i_n} = \sum_{i_1,...,i_n} a_{i_1,...,i_n} X_1^{i_1}...X_j^{i_j+1}...X_n^{i_n}$$

Cette condition devant être vérifiée pour tous les j, on doit avoir :

$$a_{i_1,...,i_n} \in \bigcap_{i=1}^{n} (\mathbb{F}_q)^{\theta_i}$$

.

Regardons à présent ce que signifie la contrainte de commutation avec les constantes. On doit avoir $aP = Pa$ c'est-à-dire :

$$P = \sum_{i_1,...,i_n} a a_{i_1,...,i_n} X_1^{i_1}...X_n^{i_n} = P = \sum_{i_1,...,i_n} \theta_1^{i_1}...\theta_n^{i_n}(a) a_{i_1,...,i_n} X_1^{i_1}...X_n^{i_n}$$

Soit p la caractéristique de $\mathbb{F}_q$ et $\theta_0(x) = x^p$. Notons $\theta_i = \theta_0^{\alpha_i}$. La condition écrite ci-dessus impose que pour tout $i_1, ..., i_n$ intervenant dans la somme (c'est-à-dire $a_{i_1,...,i_n} \neq 0$), on ait $\theta_1^{i_1}...\theta_n^{i_n} = id$, on a donc la condition suivante sur les indices :

$$\alpha_1 i_1 + ...\alpha_n i_n \equiv 0 \ [r]$$

avec $q = p^r$.

En conclusion :

$$Z(\mathbb{F}_q[\underline{X^\theta}]) = \{ \sum_{i_1,...,i_n} a_{i_1,...,i_n} X_1^{i_1}...X_n i_n, \ \alpha_1 i_1 + ...\alpha_n i_n \equiv 0 \ [r], \ a_{i_1,...,i_n} \in \bigcap_{i=1}^{n} (\mathbb{F}_q)^{\theta_i} \}$$

Références

[1] O.Öre, *On a special classe of polynomials*, Trans. Amer. Math. Soc. 1933.

[2] E.M.Gabidulin, *Theory of codes with maximum rank distance*, Russian Original Vol.21, No.1, January-March, 1985.

[3] D.Boucher, W.Geiselmann et F.Ulmer, *Skew Cyclic Codes*, Advances in Mathematics of Communications, **2**, 273-292 (2008).

[4] D.Boucher et F.Ulmer, *Coding wih skew polynomial rings*, à paraître dans : Journal of Symbolic Computation.

[5] L.Chaussade, P.Loidreau et F.Ulmer, *Skew codes of prescribed distance or rank*, à paraître dans : Designs, Codes and Cryptography.

[6] C.Rigoni, *Construction of n variable codes*, Discrete Mathematics 56 (1985) 275-280.

[7] F.Chyzak, *Fonctions holonomes en calcul formel*, Thèse universitaire no. TU 0531, INRIA. Soutenue le 27 mai 1998.

[8] M.Pesch, *Two-sided Gröbner bases in iterated Ore extensions*, MIP-9602.

[9] D.Müller, *Gröbnerbasen in Ore-Algebren*, Dissertation zur Erlangung des akademischen Grades eines Doktors der Mathematik (2006).

[10] M.Zhou et F.Winkler, *Computing difference-differential dimension polynomials by relative Gröbner bases in difference-differential modules*, Journal of Symbolic Computation (2008), doi :10.1016/j.jsc.2008.02.001.

[11] D.Cox, J.Little et D.O'Shea, *Ideals, Varieties and Algorithms*, Second Edition, Springer 1996.

[12] W.W.Adams et P.Loustaunau *An Introduction to Gröbner Bases*, American Mathematical Society1994.